

# Notice of Allowability

Application No.

09/834,106

Examiner

Pramila Parthasarathy

Applicant(s)

FENG ET AL.

Art Unit

2136

## -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12/1/2006.
2. ☒ The allowed claim(s) is/are 9-32; Renumbered as 1-24.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

### Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance.
9. ☐ Other \_\_\_\_\_

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

### **DETAILED ACTION**

1. Applicant's amendments to claims filed on December 1, 2006 has been entered and made of record.

### ***Response to Arguments***

2. Applicant's arguments with respect to the amended claims have been fully considered are persuasive.

### ***Allowable Subject Matter***

2. Claims 9 – 32 are allowed and renumbered as 1 – 24.
3. The following is an examiner's statement of reasons for allowance: The Admitted prior art Gammie et al. U.S. Patent 5,237,610 disclose a method for transmitting the encrypted keys and secret serial numbers to a plurality of broadcasters who may in turn multiplex this signal with their own program signals so that any given channel received by a subscribers contains the key and secret serial number. Furthermore, Gammie et al. disclose the program signal is scrambled with a key and the key itself is twice encrypted and multiplexed with the scrambled program signal.

However, the admitted prior arts do not disclose, teach or suggest, "generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database; encrypting the plurality of digital objects using the associated encryption keys; encrypting the plurality of encryption keys by the database; transmitting to a requester the plurality of encrypted digital objects and encryption keys; receiving from the requester at least one of the encryption keys, wherein the received encryption keys has been re-encrypted by the requester prior to transmission; generating a partially decrypted encryption key at the database by decrypting the received encryption key and transmitting the partially decrypted encryption key to the requester".

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Deborah S. Gladstein, registration number 43,636 on January 24, 2007.

IN THE CLAIMS:

13. (Amended) A method for selecting a digital object in a database, the method comprising:

- requesting a plurality of digital objects from an electronic database;
- receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;
- receiving from the database plurality of keys associated with the plurality of digital objects wherein each key has been encrypted by the database;
- selecting a ciphertext key from the plurality of received keys;
- re-encrypting the selected ciphertext key;
- transmitting the re-encrypted ciphertext key to the database;
- receiving from the database the key wherein the key has been partially decrypted by the database;
- decrypting the partially decrypted key using the second cryptography scheme to generate a decrypted key; and
- decrypting the received digital object using the decrypted key.

17. (Amended) A system for selecting a digital object in a database, the system comprising a processor for:

- generating a plurality of encryption keys, each encryption key associated with one of a plurality of digital objects stored in an electronic database;
- encrypting the plurality of digital objects using the associated encryption keys;

encrypting the plurality of encryption keys;  
transmitting to a requester the plurality of encrypted digital object and encryption keys;  
receiving from the requester at least one of the encryption keys, wherein the received encryption key has been re-encrypted by the requester prior to transmission;  
generating a partially decrypted encryption key by decrypting the received encryption key using the first cryptography scheme; and  
transmitting the partially decrypted encryption key to the requester.

21. (Amended) A system for selecting a digital object in a database, the system comprising a processor for:

requesting a plurality of digital objects from an electronic database;  
receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;  
receiving from the database plurality of keys associated with the plurality of digital objects wherein each key has been encrypted by the database;  
selecting a ciphertext key from the plurality of received keys;  
re-encrypting the selected ciphertext key;  
transmitting the re-encrypted ciphertext key to the database;  
receiving from the database the key wherein the key has been partially decrypted by the database;

decrypting the partially decrypted key using the second cryptography scheme to generate a decrypted key; and

decrypting the received digital object using the decrypted key.

29. (Amended) A machine-readable medium having program code stored thereon which, when executed by a machine, causes the machine to perform a method for selecting a digital object in a database, the method comprising:

requesting a plurality of digital objects from an electronic database;

receiving from the database the requested plurality of digital objects, wherein each digital object has been encrypted using an associated encryption key;

receiving from the database plurality of keys associated with the plurality of digital objects wherein each key has been encrypted by the database;

selecting a ciphertext key from the plurality of received keys;

re-encrypting the selected ciphertext key;

transmitting the re-encrypted ciphertext key to the database;

receiving from the database the key wherein the key has been partially decrypted by the database;

decrypting the partially decrypted key using the second cryptography scheme to generate a decrypted key; and

decrypting the received digital object using the decrypted key.

Art Unit: 2136


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

January 30, 2007.

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
2,5107